



# **Key Management Workshop**

November 1-2, 2001



## History


- ◆ Need for approved key establishment schemes for Federal applications to meet security and interoperability needs
- ◆ February 10-11, 2000 Workshop called for key management “framework” document specifying needed documents
  - Schemes including DH, RSA, and ECC from ANSI X9.42, 44, and 63 to be part of initial effort
  - At least one royalty-free scheme
  - Timeline

The government has defined a need for secure key establishment schemes.

In February of 2000, NIST a public workshop to discuss key management. The workshop recommended that:

- we develop a framework document that outlined the needed documents,
- initially include DH, RSA and EC schemes defined in ANSI documents,
- include at least one royalty-free scheme, and
- provide a timeline

This has been done and was made available last fall.




## NIST Framework Approach

- ◆ Scheme Definition Document (Standard or Recommendation)
  - DH and MQV from ANSI X9.42
  - RSA from ANSI X9.44
  - ECC from ANSI X9.63
  - Key wrapping
  - Key derivation from a master key (?)

The framework document specified the development of two documents. The first document is a schemes definition document, not to be confused with a protocol specification. This document could become either a standard or a recommendation. The initial schemes document will contain:

- DH and MQV key agreement schemes from ANSI X9.42,
- RSA key transport from ANSI X9.44,
- EC DH and MQV key agreement and key transport from ANSI X9.62,
- a key wrapping scheme, and
- may include key derivation from a master key.




## NIST Framework Approach (Contd.)

- ◆ Key Management Guidance Document (Recommendation or Guideline)
  - Key lifecycle
  - Cipher suite negotiation (selection)
  - Cryptoperiods
  - Assurance
  - Accountability
  - Key backup, archiving and recovery
  - PKI-related issues
  - Protocol issues
  - Implementation issues

The second document will be a key management guidance document, which could become either a recommendation or a guideline. The document will discuss:

- Key mgmt. from generation through destruction
- What algorithms and key sizes will be used.
- The cryptoperiods of the keys
- Assurance issues, such as domain parameter and public key validation, correct implementation.
- and a whole raft of other related issues.



## Framework Timeline


- ◆ First draft for review (June 2001)
- ◆ Proposed key wrapping scheme (July 2001)
- ◆ Workshop on first draft (October 2001)
- ◆ Continued Development (Thereafter)

The timeline in the framework document proposed a timeline for the first phase of the effort, up through this workshop, and listed other subjects to be covered thereafter. However, as with all projected timelines, it's hard to keep. However, we did get workshop documents out for review two or three weeks ago.


So...




And here we are; just about  
back on schedule!



## And so, we're here today

- ◆ Purpose of the workshop
  - This is not final!
  - We're all ears 
- ◆ Recording
- ◆ Report: <http://www.nist.gov/kms>
- ◆ Physical considerations


Workshop documents are not the final documents,  
but provide the concepts and ideas being developed.  
We're here to provide an opportunity for the public to discuss  
the direction that the key management documents are  
taking  
And to get input in areas where the document developers are  
less knowledgeable than or have a different background  
or perspective from the private sector  
Workshop will be recorded to help to develop a  
report that will be available at:  
Location of restrooms, cafeteria and break-out rooms  
(B-111 & Lecture room D)



November 1: Morning Agenda	
9:00-9:05	Welcome to the Workshop (Elaine Barker)
9:05-9:15	Overview of the History of the Key Management Project
	Goals and Purpose of Workshop
	Goals and Purpose of the Key Establishment Schemes Document (Elaine Barker)
9:15-10:15	Overview of the Key Establishment Schemes Document (Miles Smid)
10:15-10:30	Break
10:30-11:30	Issues and Discussions (Second Pass, Elaine Barker and Miles Smid)
11:30-12:30	Lunch

Today and tomorrow we'll be discussing both the Schemes and the Key Mgmt. Documents. We'll conduct two passes for each document. The first pass will be a high level overview. During the second pass, we hope that you will provide us with your views. Today's topic is the Schemes document, with Miles providing the overview, and Miles and myself jointly conducting the second pass through the document. We've planned 15 minute breaks in the morning and afternoon, and an hour for lunch.






November 1: Afternoon Agenda	
12:30-1:30	Issues and Discussion Continued (Second Pass, Elaine Barker and Miles Smid)
1:30-2:00	Final Discussion and New Items (Elaine Barker and Miles Smid)
2:00-2:15	Break
2:15-3:15	Status of Draft ANSI X9.44 (Burt Kaliski)
3:15-3:45	Future Plans (Elaine Barker)
3:45-4:00	Break
4:00-4:15	Overview of the Goals and Purpose of the Key Management Guideline (Elaine Barker)
4:15-4:45	Overview of the Key Management Guideline (Curt Barker)
4:45	Close for the day

In the afternoon, we'll have a status report on ANSI X9.44 by Burt Kaliski.

Time permitting, we'll begin the Key Mgmt. Document in the late afternoon, with an overview of the document by Curt Barker.




## November 2: Morning Agenda

9:00-9:30	Introduction, Glossary, and Acronyms (Tim Polk)
9:30-10:30	Cryptographic Algorithms, Keys, and Other Keying Material (Miles Smid)
10:30-10:45	Break
10:45-11:45	Key Management Lifecycle (Curt Barker, Miles Smid)
11:45-12:45	Lunch

Then tomorrow morning we'll start the second pass and discuss the document in more detail.

Tim Polk will begin with the introduction and glossary, followed by a discussion of the section on cryptographic keys and other keying material by Miles.

Curt will lead discussions on the majority of the lifecycle section, with Miles taking over for the key establishment section.



November 2: Afternoon Agenda	
12:45-1:45	Key Management Lifecycle Continued (Curt Barker)
1:45-2:45	General Key Management Guidance (Elaine Barker)
2:45-3:00	Break
3:00-3:30	Key Management Guidance-Selected Infrastructures (Tim Polk)
3:30-4:30	Key Management Guidance-Selected Protocols and Applications (Bill Burr)
4:30-5:00	Final Discussion and New Items (Curt Barker, Elaine Barker, Bill Burr, Tim Polk, Miles Smid)
5:00-5:15	Future Plans (Elaine Barker)
5:15	Close

I will attempt to lead us through discussions on the general Key Mgmt. Guidance section, followed by Tim discussing plans for the selected infrastructures, and Bill Burr discussing protocols and applications.

As you have see, we have a lot of material to discuss. We are scheduled to be done by about 5:00 tomorrow. If we don't have time to finish, please email us with you additional comments.



## Key Establishment Schemes

- ◆ Document developers: Elaine Barker and Miles Smid
- ◆ Goals and Purpose
  - Secure schemes
  - Validation
  - Minimize number of schemes

To provide approved secure key establishment schemes for  
Federal government applications

To provide these schemes in a manner that can be validated

To minimize the number of schemes, where reasonable